SORBA la Interacción de TLS y SRTP-RTP en el CUBO usando IOS CA

Contenido

Introducción

Este documento describe los fundamentos del Session Initiation Protocol (SIP) Transport Layer Security (TLS) y del protocolo Real-Time Transport seguro (SRTP) sobre el Cisco Unified Border Element (CUBO) con un ejemplo de configuración.

La comunicación por voz segura sobre el CUBO se puede dividir en dos porciones:

- Asegure la señalización – Aplicaciones TLS del CUBO de asegurar la señalización sobre el SORBO y la seguridad de protocolos en Internet (IPSec) para asegurar la señalización sobre H.323
- Asegure los media – SRTP

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Los archivos del administrador de las Comunicaciones unificadas de Cisco (CUCM) Certificate Trust List (Lista de confianza del certificado) (CTL) se crean para el Mezclado-MODE
- Los Teléfonos IP se registran en el modo seguro (el cifrado)
- Se hace el voip y la configuración de dial-peer básicos del servicio de voz del CUBO

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM 10.5

- CUBO – 3925E con IOS 15.3(3)M3
- Cisco IP Communicator (CIPC)

Antecedentes

- TLS - TLS y su precursor, Secure Sockets Layer (SSL), son los protocolos criptográficos que proporcionan la Seguridad de comunicación sobre Internet.

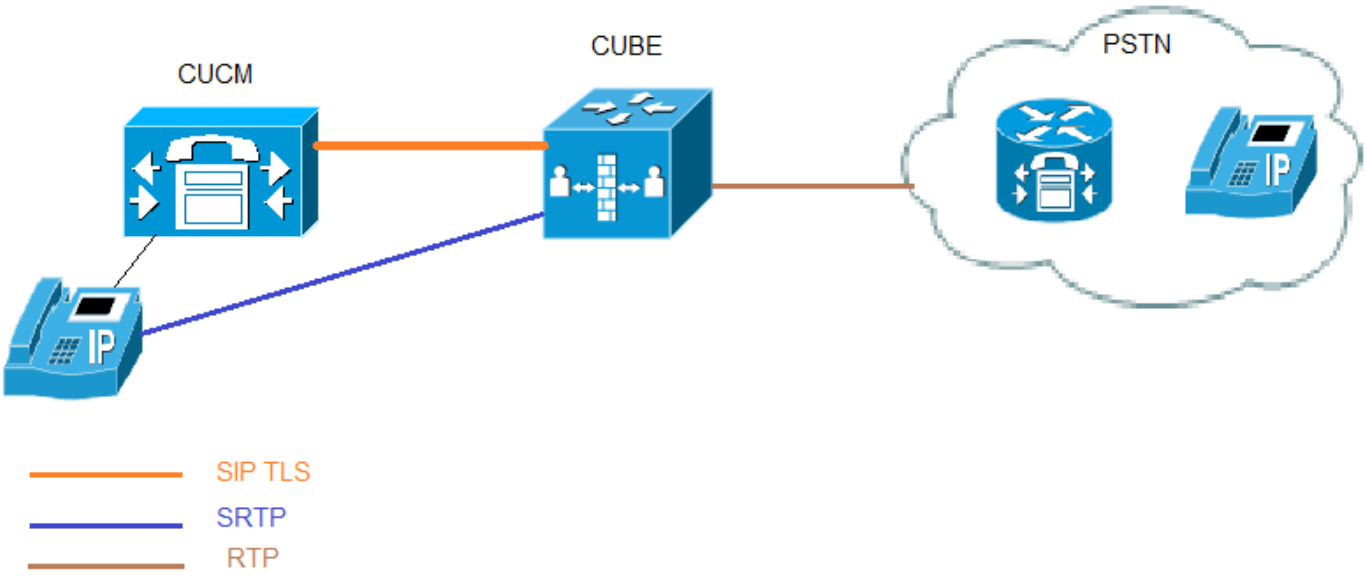
En las equivalencias del modelo del Open Systems Interconnection (OSI), TLS/SSL se inicializa en la capa 5 (la capa de sesión) y después trabaja en la capa 6 (la capa de presentación). En ambos los modelos, TLS y el SSL trabajan en nombre de la capa de transporte subyacente, cuyos segmentos llevan los datos encriptados.

- Certificate Authority (CA) - La entidad confiable esa los problemas certifica: Cisco o una entidad de tercera persona.
- Autenticación del dispositivo - Procese que valida la identidad del dispositivo y se asegura de que la entidad es lo que demanda ser antes de que se haga una conexión.
- Cifrado - Proceso de traducir los datos en el texto cifrado que asegura la confidencialidad de la información. Solamente el receptor deseado puede leer los datos. Requiere un algoritmo de encripción y una clave de encripción.
- Público/claves privadas - Claves que se utilizan en el cifrado. Las claves públicas están extensamente - disponible, pero las claves privadas son sostenidos por sus propietarios respectivos. El cifrado asimétrico combina ambos tipos.

Configurar

Diagrama de la red

En esta imagen, el ejemplo de configuración para configurar el SORBO TLS y SRTP entre el teléfono CUCM/IP y el CUBO se muestra. Internetworks del CUBO entre el SRTP y el Real-Time Transport Protocol (RTP). El CUBO actúa como IOS CA y CUCM utilizaría los certificados autofirmados.



Configuración del CUBO

1. Reloj de la configuración y servidor HTTP del permiso

Sincronice los relojes en el servidor y el trustpoints del cliente (CUBE/OGW/TGW) de CA. Si no, hay problemas con la validez de los Certificados publicados por el servidor de CA.

```
Secure-CUBE#clock set <hh:mm:ss> < Day of the month> <MONTH> <Year>
Or
Ntp server <IP Address>
```

Uso HTTP del trustpoints del cliente de recibir el certificado de CA.

```
Secure-CUBE(config)#ip http server
```

2. Genere un par de claves RSA

Este paso genera el soldado y las claves públicas.

En este ejemplo, el CUBO es apenas una escritura de la etiqueta. Puede ser cualquier cosa.

```
Secure-CUBE(config)#crypto key generate rsa general-keys label CUBE modulus 1024
The name for the keys will be: CUBE
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Secure-CUBE(config)#
```

3. Servidor IOS CA de la configuración

En este ejemplo, el servidor de CA se nombra cubo-Ca.

```
crypto pki server cube-ca
database level complete
no database archive
grant auto
lifetime certificate 1800

Secure-CUBE(cs-server)#no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password:

Re-enter password:

% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

% Certificate Server enabled.

Secure-CUBE(cs-server)#
```

4. Cree el trustpoints PKI para el cubo para la comunicación de TLS.

En este ejemplo, el nombre del trustpoint para el CUBO es CUBE-TLS. La dirección IP usada en el URL de la inscripción debe ser interfaz local en el CUBO. El asunto usado en este paso debe hacer juego en el asunto X.509 en el perfil de seguridad del trunk del SORBO CUCM. La mejor práctica es utilizar el hostname con el Domain Name (si se habilita el Domain Name).

Par clave del socio RSA creado en el paso 2.

```
crypto pki trustpoint CUBE-TLS
enrollment url http://X.X.X.X:80
serial-number none
fqdn none
ip-address none
subject-name CN=Secure-CUBE
revocation-check none
rsakeypair CUBE
```

5. Autentique el trustpoint con el servidor de CA y valide el certificado de CA.

```
Secure-CUBE(config)#crypto pki authenticate CUBE-TLS
Certificate has the following attributes:
      Fingerprint MD5: BCEBB5A1 1AC882F7 24BE476D 06537711
    Fingerprint SHA1: CE2FEEA5 42515B33 3EF6A8F6 7E31D6DF 8E32BEB6

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Secure-CUBE(config)#
```

6. Aliste el trustpoint con el servidor de CA.

En este paso el CUBO recibe un certificado firmado de CA.

```
Secure-CUBE(config)#crypto pki enroll CUBE-TLS
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:


% The subject name in the certificate will include: CN=Secure-CUBE
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CUBE-TLS' commandwill show the fingerprint.

Secure-CUBE(config)#
```

7. Cree el trustpoint para el CUCM.

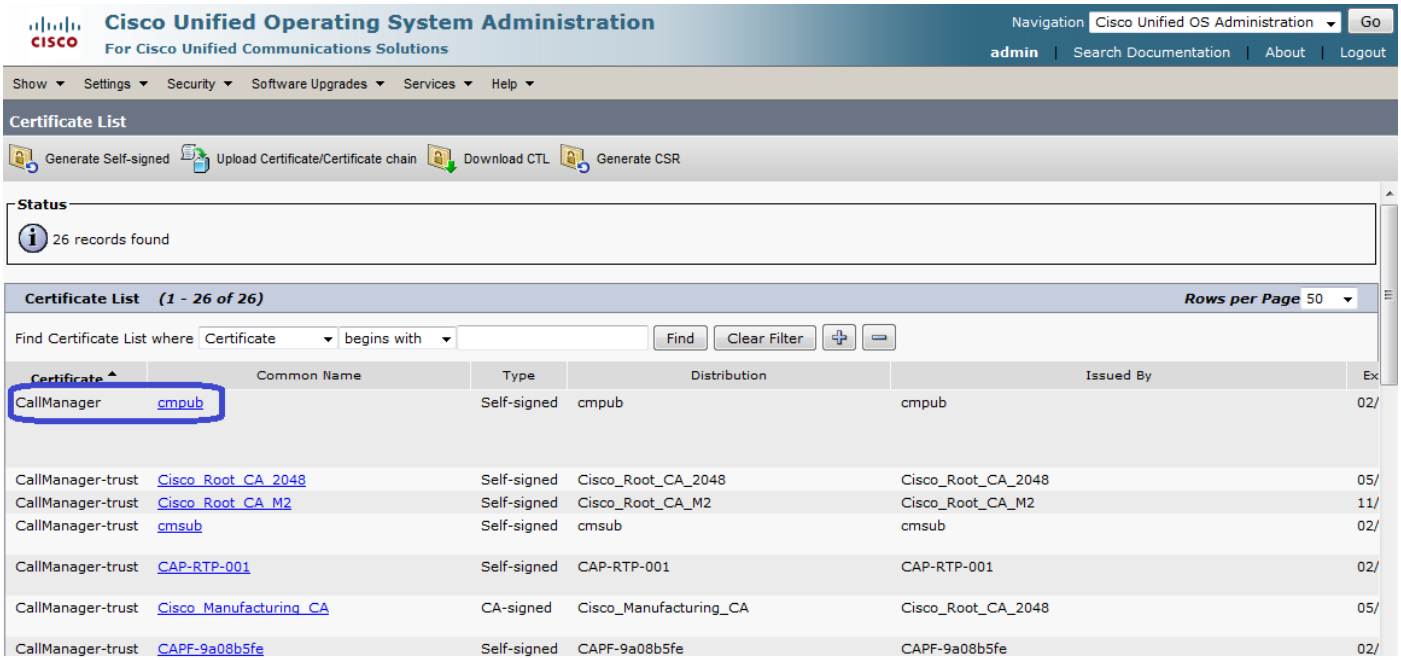
Si el grupo de CallManager tiene los servidores CM múltiples, después el trustpoint necesita ser creado para todos los servidores, si no la Conmutación por falla no trabaja.

```
crypto pki trustpoint cucmpub
 enrollment terminal
 revocation-check none

crypto pki trustpoint cucmsub
 enrollment terminal
 revocation-check none
```

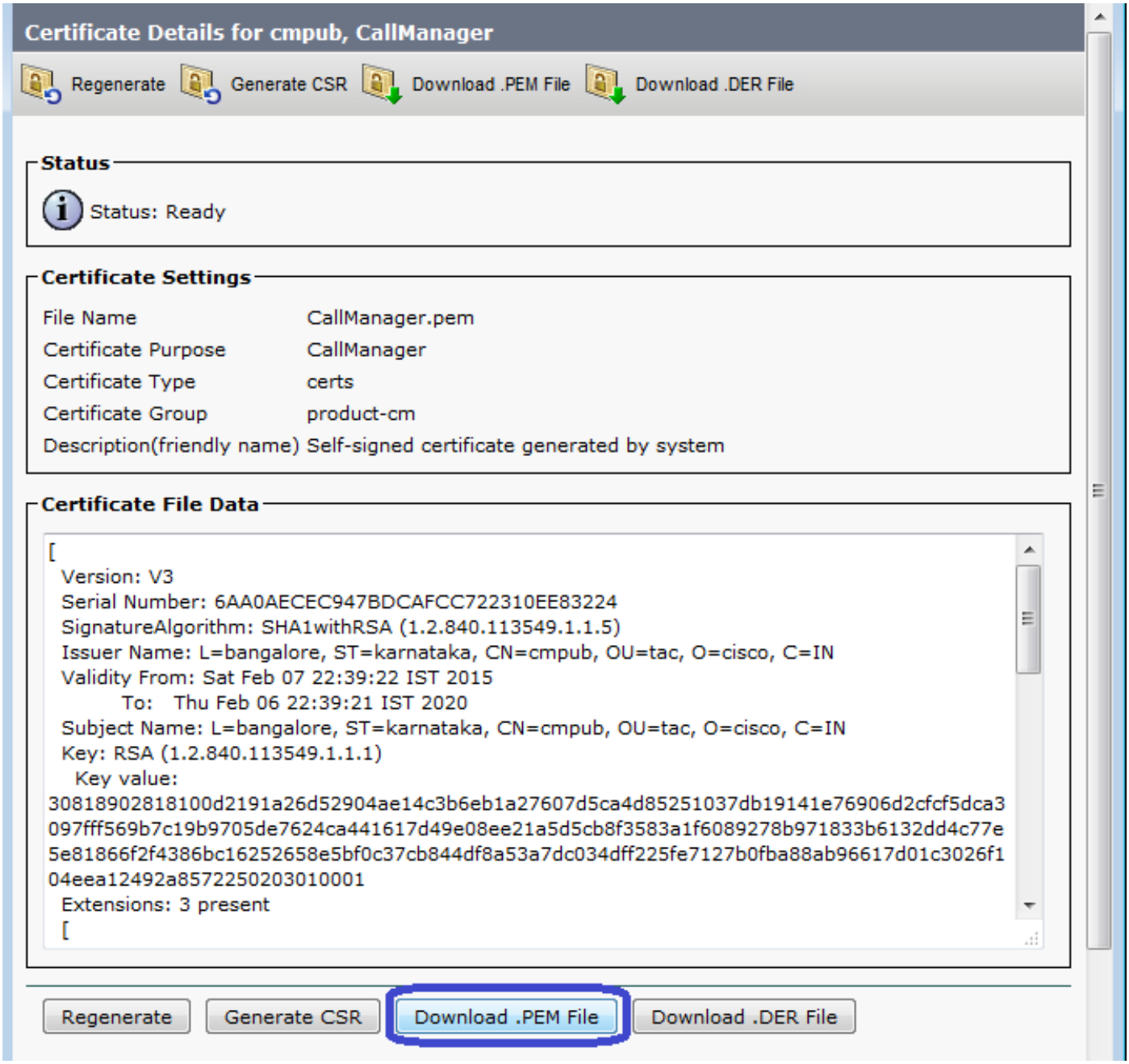
8. Aliste el certificado CUCM PARA CUBICAR.

Paso 1. Login a CUCM OS admin.

Paso 2. Navegue al **Certificate Management (Administración de certificados) > al hallazgo de la Seguridad.**



Paso 3. Haga clic el certificado del **CallManager**, después descargue y salve el archivo del .PEM tal y como se muestra en de esta imagen.



Paso 4. Abra el archivo en la libreta y copie el contenido del COMIENZAN EL CERTIFICADO PARA TERMINAR EL CERTIFICADO.

Paso 5. Pegue este certificado en el CUBO como se muestra.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
```

```
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

Paso 6. Siga el mismo procedimiento para los otros servidores CUCM.

9. Configure TCP TLS como Transport Protocol.

Esto se puede hacer en un global o en un dial-peer llano.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

10. Asigne el trustpoint para el sorbo-UA, este trustpoint se utiliza para toda la señalización del SORBO entre el CUBO y CUCM

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
```

```
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

u omita el trustpoint puede ser configurado para toda la señalización del SORBO del CUBO.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

11. Habilite el SRTP.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

12. Para la Interacción SRTP y RTP, se requiere el transcoder seguro.

Si la versión de IOS es 15.2.2T (CUBO 9.0) o más adelante entonces, transcoder LTI puede ser configuración para minimizar la configuración.

El transcoder LTI no necesita la configuración del trustpoint PKI para las llamadas SRTP-RTP

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
```

```
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

Si el IOS está debajo de 15.2.2T, después transcoder del sccp de la configuración.

El transcoder del Skinny Call Control Protocol (SCCP) necesitaría el trustpoint para señalar sin embargo si utilizan al mismo router para recibir el transcoder entonces que el mismo trustpoint (CUBE-TLS) se puede utilizar para el CUBO así como el transcoder.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

Configuración CUCM

1. Certificado IOS del CUBO de la exportación a CUCM.

Paso 1. Certificado IOS de la exportación. Copie el certificado de CA uno mismo-firmado y sálvelo como archivo del .PEM por ejemplo, Secure-CUBE.pem

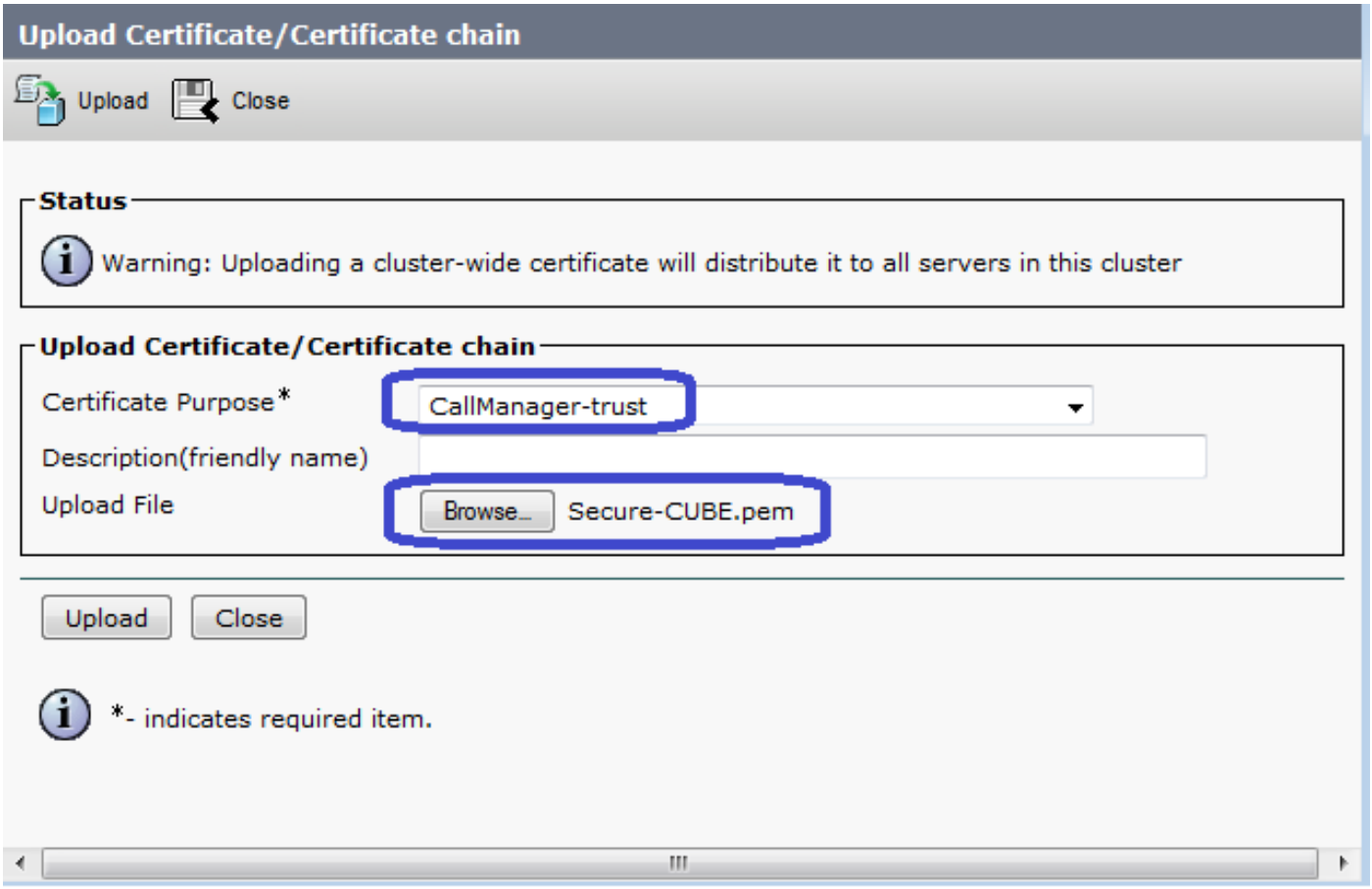
```
 Secure-CUBE(config)#crypto pki export CUBE-TLS pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEyNTYyMVoXDTE4MDIxMDEyNTYyMVowEjEQMA4GA1UEAxMH
```

```
Y3ViZS1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtN3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr0lvbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnv1MH32lJ5tVzAPHj9z7GdD42+gZSoHqOMlFB8z4+VDPzpoxpswI
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUnqzvazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6l84ZKE4gBBQr7DfK8MA0GCSqGSIb3DQEBBAUAA4GB
AEfnNrB4nls81vz0cqlpuTjID+KVyKRwYNP04zJYWCV7P+mlbpMfC/qh14z5/RzL
e5Bq6NUnxWByLR4gcFjmdSlE6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
CEnHng0AvcTRv/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB7TCCAVagAwIBAgIBAjANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEzMDI1MFoXDTE4MDIxMDEyNTYyMVowFjEUMBIGA1UEAxML
U2VjdXJlLUNVQkUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKWtfO
F9bBVYhVwQK8y2c5NMkJCY//pisg+oforvxalPKAXj/jqDkqtDTc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTwk5jf9+YGIMVsivbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAf
BgNVHSMEGDAWgBSerO9rMr/upfOGShOIAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOWVf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXxAOTHhOsEbm/vfqk2vbYiHUO9AtDDI+kNecSuOGmd7fokJMP9K1xc1i2a
vrr2qwQYqRAh68BwTjWzR3mFAGbDZZwiywv1jJ92ra3EMAUc0sJZSLzGY0+BjO/E
dEW6JUIOx3NxP2SBN1NMAQ0=
-----END CERTIFICATE-----

Secure-CUBE(config)#
```

Paso 2. Certificado de CA IOS de la carga en CUCM como CallManager-confianza.

Paso 3. Navegue al **Certificate Management (Administración de certificados) del > Security (Seguridad) de la administración CM OS > al certificado/a la Cadena de certificados de la carga**

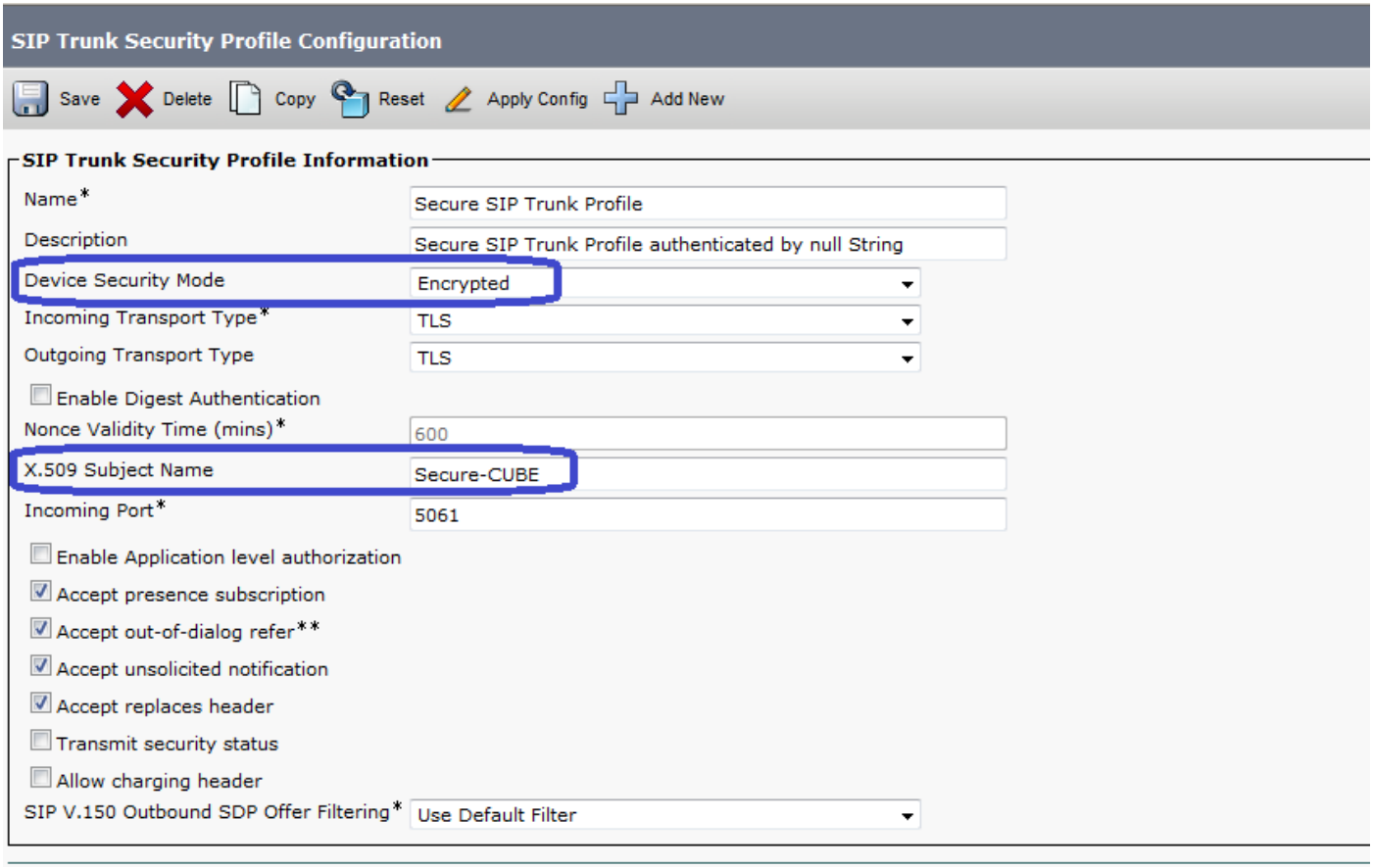
Paso 4. Archivo del .PEM de la carga tal y como se muestra en de esta imagen.



2. Cree el nuevo perfil de seguridad del trunk del SORBO

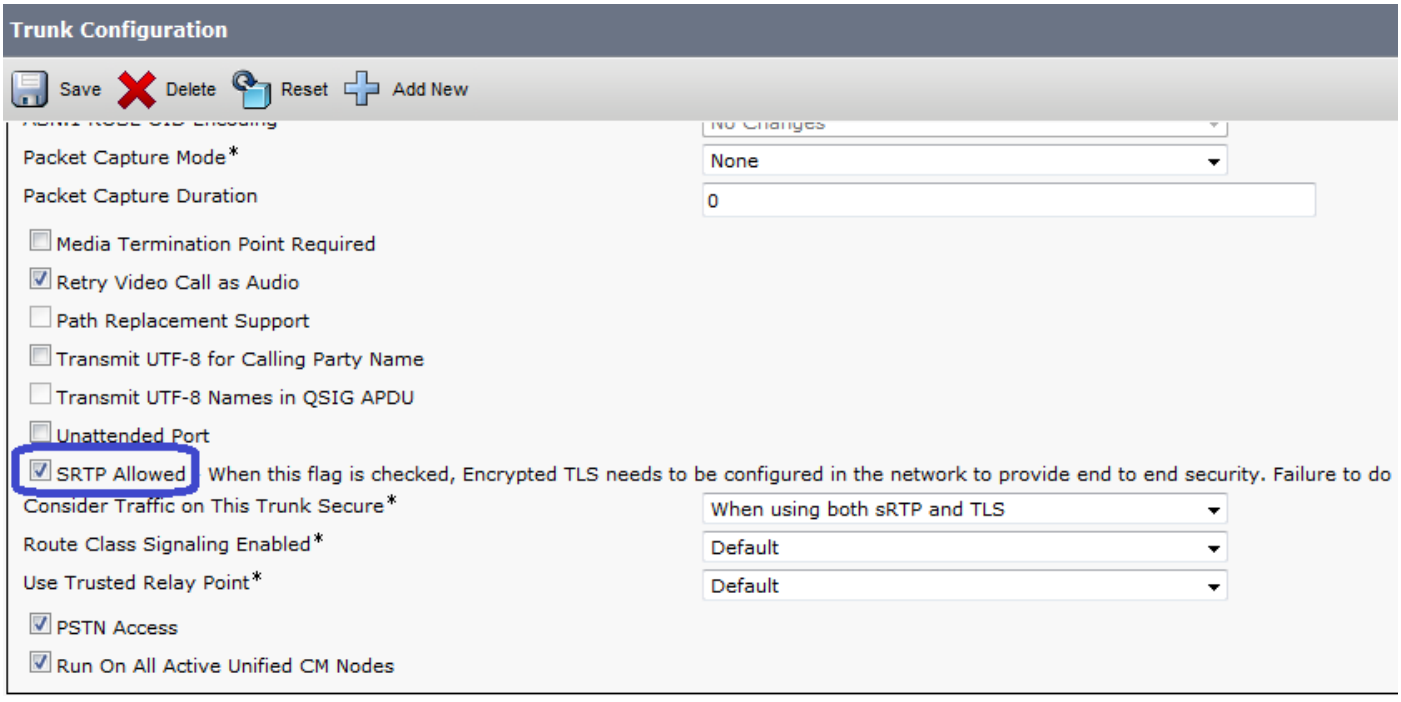
Paso 1. En la administración CM navegue al **> Security (Seguridad) del sistema > a los perfiles de seguridad > al archivo del trunk del SORBO.**

Paso 2. Copie la existencia **perfil no seguro del trunk del SORBO** para crear el nuevo perfil seguro tal y como se muestra en de esta imagen.

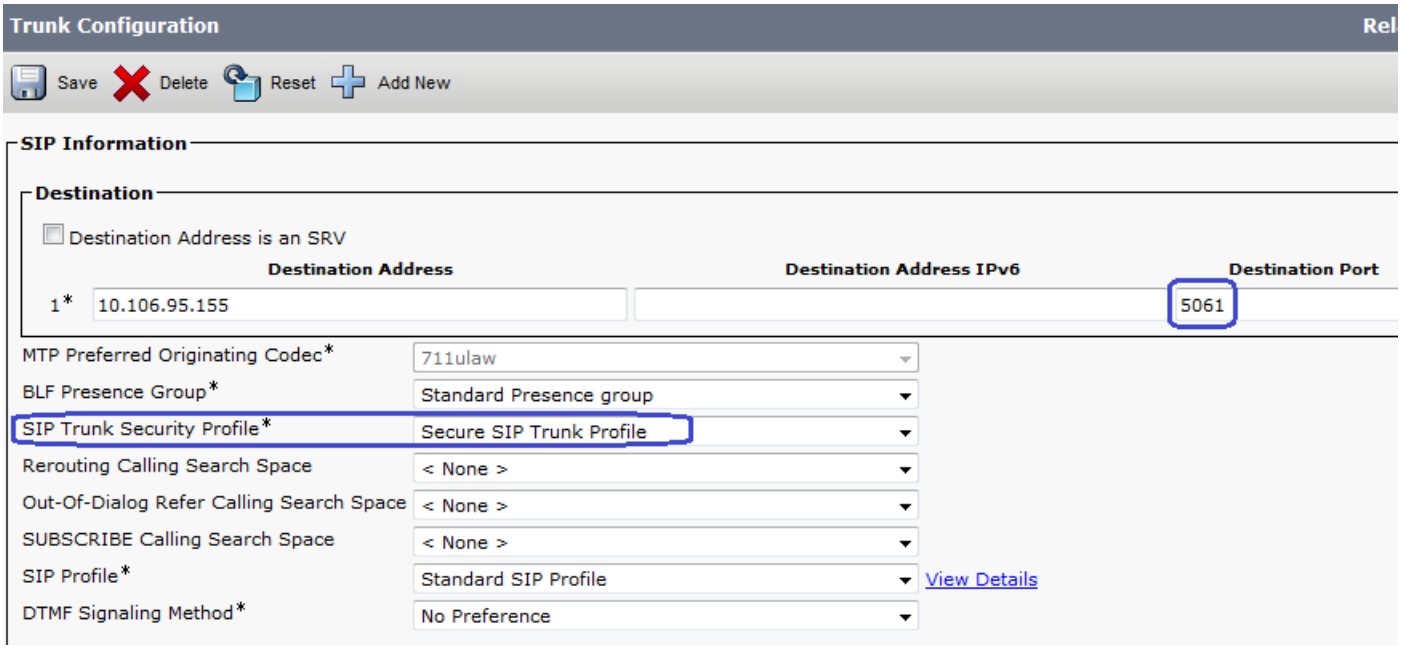


3. Cree el trunk del SORBO al CUBO

Paso 1. Habilite el SRTP en el trunk del SORBO tal y como se muestra en de esta imagen.



Paso 2. Configure el puerto destino 5061 (TLS) y aplique nuevo aseguran el perfil de seguridad del trunk del SORBO en el trunk del SORBO tal y como se muestra en de esta imagen.



Verificación

```
Secure-CUBE#show sip-ua connections tcp tls detail
Total active connections : 2
No. of send failures : 0
No. of remote closures : 13
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition

Remote-Agent:10.106.95.151, Connections-Count:2
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
=========== ======= =========== =========== ===========
5061 16 Established 0 10.106.95.155
57396 17 Established 0 10.106.95.155


-------------- SIP Transport Layer Listen Sockets ---------------
Conn-Id Local-Address
=========== ============================
2 [10.106.95.155]:5061
```

La salida de la descripción de la voz activa de la llamada de la demostración se captura cuando se utiliza el transcoder LTI.

```
Secure-CUBE#show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

También cuando una llamada cifrada SRTP se hace entre el Cisco IP Phone y CUBO o gateway, un icono del bloqueo se visualiza en el teléfono del IP.

Troubleshooting

Estos debugs son útiles para resolver problemas los problemas PKI/TLS/SIP/SRTP.


```
Secure-CUBE#show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```